Software Version Description for

Electronic Commerce Processing Node

Update 2.2.0.5

August 1999

Inter-National Research Institute, Inc.
12350 Jefferson Avenue, Suite 400
Newport News, Virginia 23602

The following trademarks and registered trademarks are mentioned in this document. Within the text of this document, the appropriate symbol for a trademark (™) or a registered trademark (®) appears after the first occurrence of each item.

UNIX is a registered trademark of The Open Group.

Software Version Description for ECPN

Contents

List of Figures

This page has been intentionally left blank.

1.0 Scope

This Software Version Description (SVD) applies to Update 2.2.0.5 of Electronic Commerce Processing Node (ECPN). This document follows the standards set forth in *Military Standard Software Development and Documentation* (MIL-STD-498) and in the *Data Item Description (DID) for a Software Version Description* (DI-IPSC-81442), as tailored by Inter-National Research Institute (INRI).

1.1 Identification

ECPN is a Computer Software Configuration Item (CSCI) of the system identified as Electronic Commerce/Electronic Data Interchange (EC/EDI).

1.2 System Overview

ECPN is being developed by INRI for the Defense Information Systems Agency (DISA). The role of ECPN is to serve as a single interface between the Government and its commercial trading partners for conducting EC/EDI. ECPN must ensure interoperability, economies of scale, and compliance to standards set forth by the Department of Defense (DoD) and Federal Program Office (PO).

The functional objectives of ECPN are to:

- Provide rigorous end-to-end accountability within the ECPN system, with no single point of failure that could result in loss or nondelivery of data
- Implement a Relational Database Management System (RDBMS) for storage of data passing through the ECPN
- Provide automated archive and retrieval mechanisms for messages and system configuration data
- Provide system performance information, including transaction statistics and communications status

1.3 Document Overview

The purpose of this document is to identify and describe the changes made to the ECPN CSCI in Update 2.2.0.5. (For descriptions of these changes, see Section 3.3.) This SVD also identifies any software problems that were corrected by the changes made in Update 2.2.0.5.

This document contains the following sections:

Scope

States the purpose of the EC/EDI system, describes the role of ECPN within EC/EDI, and states the purpose of this SVD. (Section 1.0)

Referenced Documents

Lists the documents applicable to this SVD. (Section 2.0)

Version Description

Lists the following items: changes made to ECPN for Update 2.2.0.5, materials that compose this release of software, possible problems and known errors with ECPN Update 2.2.0.5. (Section 3.0)

Notes

Defines the acronyms and abbreviations used in this SVD. (Section 4.0)

2.0 Referenced Documents

The following documents are referenced in this SVD. In the event of a later version of a referenced document being issued, the later version shall supersede the referenced version.

- *Data Item Description – Software Version Description* (DI-IPSC-81442), December 1994.
- *Military Standard – Software Development and Documentation* (MIL-STD-498), December 1994.
- *Software User's Guide for Electronic Commerce Processing Node, Version 2.2,* June 1999.
- *System Administrator's Guide for Electronic Commerce Processing Node, Version 2.2,* June 1999.

3.0 Version Description

The following subsections describe ECPN Update 2.2.0.5.

3.1 Inventory of Materials Released

The following physical media and associated documentation compose ECPN Update 2.2.0.5.

Software

- Electronic Commerce Processing Node, 2.2.0.5 Update Tape.

Documentation

- *Software Version Description for Electronic Commerce Processing Node Update 2.2.0.5*, August 1999.

3.2 Inventory of Software Contents

This section has been tailored out.

3.3 Changes Installed

The following software changes were integrated in ECPN Update 2.2.0.5. This information is grouped according to the following categories:

- Audit/Logging
- Communications
- Databases
- Message Processing/Routing
- Security
- Translation

Audit/Logging

1. *Problem:* In the Channel File Viewer of the outgoing channel log, the data is not aligned with the column headers.

   Solution: Aligned data with the column headers.

2. *Problem:* Attachments to email messages (e.g., traffic reports with MIME encoding) are not shown in the outgoing channel log.

   Solution: Modified email_send to display the entire text of an email message.

3. *Enhancement:* Traffic reports may now be produced for a specific UDF message type. For instructions on generating traffic reports, see Appendix J of the *System Administrator's Guide for Electronic Commerce Processing Node*. The instructions for configuring a channel to transmit traffic reports, located in Section 4.1.3 of the *Software User's Guide for Electronic Commerce Processing Node*, should be replaced with the instructions provided in Appendix A of this document.

Communications

1. *Problem:* The View Columns dialog box (opened through the Communications Manager) has "_popup" in its title bar.

   Solution: Removed "_popup" from the title bar.

2. *Problem:* In alert notification messages and the output produced from the Print menu option of the Communications Manager, the channel name is truncated.

   Solution: Modified these applications to display the full channel name.

3. *Enhancement:* Added the following items to the status bar of the Communications Status window:

   - Number of channels down
   - Time since a channel received a message
   - Time since a channel transmitted a message

4. *Problem:* The File Transfer Protocol Daemon (ftpd) does not generate an alert when it receives a zero-length file.

   Solution: Modified ftpd to generate an alert when a zero-length file is received.

5. *Problem:* When a channel is added to the communications channel database, an invalid error message is placed in the RPCServer's session log.

   Solution: Modified the RPCServer so that the invalid error message is not generated when a channel is added.

6. *Problem:* Shortly after ECPN is started, the Communications Manager fails to open.

   Solution: The problem is caused by a brief period in which the RPCServer is alive but still initializing. Modified the Communications Manager to handle this condition correctly.

7. *Enhancement:* For the Electronic Commerce Data Warehouse (ECDW) program, added daily translation logs and the GTN Standard Carrier Alpha Code (SCAC) table to the list of files sent each day to the Data Warehouse.

8. *Enhancement:* Added secure copy (SCP) as an interface for channels. Instructions for using this interface are provided in Appendix B of this document.

Databases

Enhancement: Some trading partner data received from the Central Contractor Registration (CCR) contains invalid values in the ISA ADDRESS and GS ADDRESS fields. Added the TPDB_ReplaceField application, which searches the trading partner database for these specific values, replacing them with the generic value, VENDOR. To run the application manually, enter the following at the command prompt:

```
/h/EC/progs/TPDB_ReplaceField
```

The system administrator may configure the application to run automatically as a cron job. Set the cron job to run periodically, depending on how often you receive data from CCR.

Message Processing/Routing

1. *Problem:* The router takes too long to route messages.

   Solution: Optimized reply route lookups and file removals to provide better performance.

2. *Problem:* An email message cannot be rerouted successfully when a new email address is added to the route.

   Solution: Modified the router to correctly handle rerouting of email messages when a new email address is added to a route.

3. *Problem:* When a message fails because it does not have a primary route, the JDS Viewer highlights some portion of the GS line as the errored portion. Because different types of GS routes are available, the highlighting is confusing.

   Solution: Modified the JDS Viewer to highlight the initial portion of the GS line.

Security

1. *Problem:* RemoteECPN fails if a user logs in with an account that does not have roles and then changes users to one that does have roles.

   Solution: Modified RemoteECPN to operate on the current user information instead of the login information.

2. *Problem:* Programs that are run as cron jobs may be run as a user (e.g., root), but the output from the cron jobs cannot be modified by another user, such as the ecpn user.

   Solution: Modified these programs so that they are now setuid ecpn.

Translation

1. *Problem:* The Defense Travel System (DTS) batch header and trailer are not enclosed in quotation marks, as required by the DTS specification.

   Solution: Modified the outgoing message formatting to enclose the DTS batch header and trailer in quotation marks.

2. *Enhancement:* Modified ECPN to allow NATO CAGE codes in the trading partner database, in addition to standard CAGE codes.

3. *Enhancement:* The GTN message type business rules require an alternative output format for transactions that cannot be translated properly using the X12 to UDF maps because of syntax or semantic errors. This alternate output is produced by a separate X12 to UDF map. The ECPN translation system has been enhanced so that the GTN default X12 to UDF map can identify data that requires alternate translation and invoke the alternate map to process that data.

4. *Problem:* A channel with an invalid message type (e.g., one that has been removed from a new map segment) cannot be edited.

   Solution: Modified the Communications Manager so that channels with an invalid message type default to X12 and can be edited.

5. *Problem:* While waiting for new messages, the translators do not catch signals.

   Solution: Modified the translators so that they no longer block signals while waiting for new messages.

3.4 Adaptation Data

The ECPN CSCI is the same for all sites. Adaptation of ECPN software is completely driven by configuration files. All adaptation data is stored in files that are read by ECPN when configuring the system for a site. These configuration files are resident on the tape used in the initial installation process.

3.5 Related Documents

In addition to the documents released with ECPN Update 2.2.0.5 (listed in Section 3.1), the following documents are pertinent to the ECPN CSCI. In the event of a later version of a document being issued, the later version shall supersede the referenced version.

- *Security Manager's Guide for Electronic Commerce Processing Node, Version 2.2,* June 1999.
- *Software Design Description for Electronic Commerce Processing Node, Version 2.2,* INRI, June 1999.
- *Software Requirements Specification for Electronic Commerce Processing Node, Version 2.2,* INRI, April 1999.
- *Software Test Plan for Electronic Commerce Processing Node, Version 2.2,* INRI, April 1999.

3.6 Installation Instructions

Follow the instructions below to install ECPN Update 2.2.0.5.

1. **Important:** This software will not install correctly if ECPN processes that will be replaced are running during the installation. To stop ECPN processes, select Stop ECPN Software from the SA Default role's Software menu.

2. Log in to the UNIX® system as `root`.

3. Determine if any of the ECPN boot processes (MenuExec, AlertDaemon, AdmMgr, AlertNotifier, and COEExecMgr) are running by entering the following commands and pressing [Enter] after each command:

   ```
   #  ps -ef | grep MenuExec
   #  ps -ef | grep AlertDaemon
   #  ps -ef | grep AdmMgr
   #  ps -ef | grep AlertNotifier
   #  ps -ef | grep COEExecMgr
   ```

   If any of these processes are running, the system returns the process identification number (PID). Enter the following command to kill each process:

   # `kill` <MenuExec PID> <AlertDaemon PID> <AdmMgr PID> <AlertNotifier PID> <COEExecMgr PID>

   (Note: Enter the process identification number of the processes, without the angle braces.)

4. To prevent any FTP sessions from starting during the installation, the FTP daemon must be disabled as follows:

   a. In the /etc/inetd.conf file, insert a # symbol at the beginning of the following line:

      ```
      ftp  stream tcp nowait root /h/EC/progs/ftpd
      ```

   b. At the command prompt, enter the following command and press [Enter]:

      ```
      #   inetd -c
      ```

5. To determine if any FTP daemon processes are currently running, enter the following command:

   ```
   #  ps -ef | grep ftpd
   ```

   If any of these processes are running, the system returns the PID. Enter the following command to kill each process:

   ```
   #  kill <PID>
   ```

   (Note: Enter the process identification number of the process, without the angle braces.)

6. Insert the 2.2.0.5 Update Tape into the tape drive. Extract the contents of the tape to a temporary directory by entering the following commands and pressing [Enter] after each command:

   ```
   #  mkdir /h/2.2.0.5

   #  cd /h/2.2.0.5

   #  tar xvf <tape drive>
   ```

   (Note: <tape drive> specifies the drive containing the 2.2.0.5 Update Tape. Enter the name of the drive, without the angle braces.)

7. To run the PostInstall application (which installs the new software), enter the following commands in order, pressing [Enter] after each command:

   ```
   #  chmod +x ./PostInstall

   #  ./PostInstall
   ```

   When the PostInstall application finishes, Update 2.2.0.5 is installed.

8. Enable the FTP daemon as follows:

   In the /etc/inetd.conf file, remove the # symbol (that you inserted in *Step 4*) at the beginning of the following line:

   ```
   #  ftp stream tcp nowait root /h/EC/progs/ftpd
   ```

   When the system is rebooted in *Step 9*, the FTP service will be re-enabled.

9. To restart the boot processes, reboot the machine.

10. Login as `ecpn`, and restart the ECPN software.

> **NOTE:** This SVD and the software media should be stored in a safe location in case it is necessary to reload the ECPN software.

3.7 Possible Problems and Known Errors

1. *Problem:* Acknowledging alerts in the Non-Urgent Alert window or opening the Alert Display Filter window can occasionally cause the alert GUIs to deadlock.

   Work-around: Exit the Non-Urgent Alert window or the Alert Display Filter window. If the system is not restored to normal, open a terminal window and kill the AlertNonInterrupt process.

2. *Problem:* Acknowledging all red alerts from the Non-Urgent Alert window may result in the ECPN GUIs locking up.

   Work-around: None.

3. *Problem:* The AlertDaemon sometimes stops processing alerts.

   Work-around: Use the check_alerts program to find out if the AlertDaemon has stopped. If the program determines that AlertDaemon has stopped processing, the program suggests a system reboot.

4.0 Notes

The following acronyms and abbreviations appear in this document:

CCR: Central Contractor Registration

COE: Common Operating Environment

CSCI: Computer Software Configuration Item

DID: Data Item Description

DISA: Defense Information Systems Agency

DoD: Department of Defense

DTS: Defense Travel System

EC/EDI: Electronic Commerce/Electronic Data Interchange

ECPN: Electronic Commerce Processing Node

FTP: File Transfer Protocol

INRI: Inter-National Research Institute

PO: Program Office

RDBMS: Relational Database Management System

SCP: Secure Copy

SSH: Secure SHell

SVD: Software Version Description

UDF: User Defined File

Appendix A Administration Settings

The ADMIN tab in the edit channel window enables you to configure the channel to transmit traffic reports and 997 and 824 acknowledgments to specific sites.

Figure A-1 Edit Channel Window: ADMIN Tab

To configure a channel to transmit traffic reports

Traffic reports (also known as message reports) contain information about the channel's daily activity. For all channels (X12 and UDF), you may transmit an X12 traffic report. For UDF channels, the X12 traffic report contains information about either the incoming X12 messages (*after* translation) or outgoing X12 messages (*before* translation). A sample X12 traffic report is provided in Appendix E of the *Software User's Guide for Electronic Commerce Processing Node*.

For some UDF channels (depending on their message type), you may transmit additional traffic reports. For example, the Daily Data Timeliness traffic report is available for the Global Transportation Network (GTN) message type. For a list of available traffic reports for a particular message type, see the DESCRIPTION box of the TRANSLATION tab of the edit channel window.

The system automatically collects traffic report data for each channel on a daily basis. When the MsgReporter utility is run (as described in Appendix J of the *System Administrator's Guide for Electronic Commerce Processing Node*), this data is generated into traffic reports. If the MsgReporter utility does not run, traffic reports are not generated; however, the report data is still collected and stored on the system. The list of files generated for X12 traffic reports and

the directory where they are stored are provided in Appendix J of the *System Administrator's Guide for Electronic Commerce Processing Node*. The list of files generated for traffic reports for a UDF message type and the directory where they are stored are provided in the DESCRIPTION box of the TRANSLATION tab of the edit channel window.

1. In the edit channel window, click the ADMIN tab (Figure A-1). The traffic reports available for the channel are listed by name in the REPORTS box, along with the method of transmission (Email or Channel), frequency of reporting (Daily or Weekly), and status (On or Off) for each report.

2. In the REPORTS box, double-click the traffic report you wish to configure. The Edit Report dialog box appears.

Figure A-2 Edit Report Dialog Box

   a. Select the Enabled check box.

   b. To specify how to send the traffic report, select one of the following Send To option buttons:

      - Channel – Sends each traffic report back to the sender on the channel for which the report is generated.

      - Email – Sends each traffic report in the form of an email message. In the Address List field, enter each email address to which the traffic report should be sent, using commas to separate each address.

   c. Click OK.

3. To save your changes, click OK. The changes will go into effect when the next communications session is initiated.

Appendix B SSH and SCP Settings

This appendix explains how to do the following:

- Configure Secure SHell (SSH)
- Add an SCP channel
- Configure an SCP channel
  - View and edit SCP remote login information
  - View and edit SSH configuration options
  - View and edit SCP transfer parameters

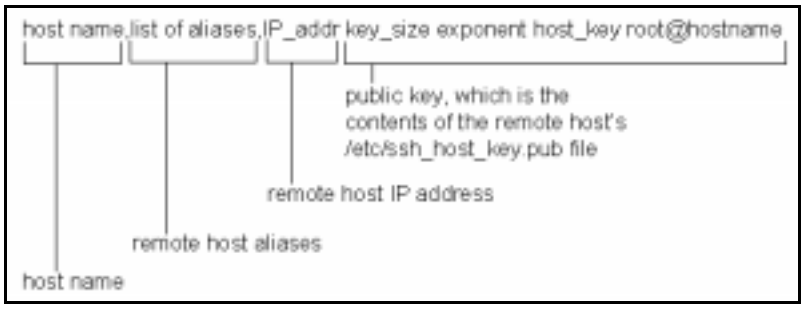
To configure Secure SHell (SSH)

The Secure Copy (SCP) interface copies files between hosts, using Secure SHell (SSH) to provide secure, encrypted communications. Before configuring the SCP interface and SSH, you must set up a public configuration file.

1. With a text editor, open the `/etc/ssh_known_hosts` file. If the file does not exist, create it.

2. In the file, edit or make an entry for each remote host with which you want to connect. For each entry, use the format shown in Figure B-1. If you have entries for more than one remote host, place a carriage return between each entry.

Figure B-1 Format of ssh_known_hosts File



The public key of the remote host must be placed in the ssh_known_hosts file in its entirety. The host_key portion of the file cannot contain any carriage returns: It must be one continuous line, just as it is on the remote host.

The following is an example of an entry in the ssh_known_hosts file:

```
k410,k410.ecpn.nn.inri.com,198.180.218.236 1024 41
13755218339270543311333756207348718277948194064748290086630
77006651388623796945142050882947379044494547735105616498299
67573383566558150760377911419791027787291599672340721530249
51960034028329194193579716687828066888697451238534412640837
30439374558213613330306197745081886656953122877620393915220
77468153589203 root@k410
```

To add an SCP channel

Add a channel as directed in Section 4.1 of the *Software User's Guide for Electronic Commerce Processing Node*. In the Interface list, select SCP.

To configure an SCP channel

The Secure Copy (SCP) interface copies files between hosts, using Secure SHell (SSH) to provide secure, encrypted communications. You can view or modify the settings that are unique to the SCP interface by choosing the SCP and SCP TRANSFER tabs within the edit channel window. The SCP tab enables you to view and edit the SCP login information and view and edit SSH configuration options. The SCP TRANSFER tab enables you to view and edit the file transfer options for the channel. To determine which options to specify for the SCP interface and SSH, coordinate with the remote site for which you are processing messages.

To view and edit SCP remote login information

IMPORTANT: To log in to the remote host, the remote host *must* allow client SSH Version 1.x connections.

1. In the edit channel window, click the SCP tab.

Figure B-2 Edit Channel Window: SCP Tab

2. In the HOSTNAME/IP ADDR field, enter either the fully qualified host name or numeric Internet Protocol (IP) address of the remote host.

3. In the LOGIN NAME field, enter the login name designated for SCP login use at the remote host.

4. In the PASSWORD field, enter the password for the specified login name at the remote host.

5. To save your changes, click OK. The changes will go into effect when the next communications session is initiated.

To view and edit SSH configuration options

1. In the edit channel window, click the SCP tab (shown in Figure B-2).

2. In the CONFIG-FILE OPTIONS box, click the CIPHER TYPE list box and select an entry from the list (either Triple-DES, Blowfish, DES, or IDEA) to specify a cipher type. The cipher type indicates the type of encryption used for the communications session.

3. Select or clear the COMPRESSION check box to indicate whether data should be compressed. If compression is selected, click the COMPRESSION LEVEL list box and select the level of compression. The levels range between 1 and 9. Level 1 provides the fastest compression, and level 9 provides the slowest compression. A higher compression level provides the best compression of data and is good for slow links (saves bandwidth) and fast machines.

4. Under AUTHENTICATION METHOD, select or clear the RHOSTS, RSA, and TIS check boxes to indicate which authentication method(s) to use. When SSH establishes a secure connection between the SSH client (ECPN) and the SSH server (remote host), SSH authenticates that the client is allowed to connect to the server, using one or more of the methods specified in these check boxes.

   - Select the RHOSTS check box to use rhosts authentication (provided that the remote server permits rhosts authentication). Using the rhosts authentication may lengthen the authentication time on slow connections.

   - Select the RSA check box to use RSA authentication.

   - Select the TIS check box to use TIS authentication. TIS authentication is performed by the remote server; thus, the remote server must have a TIS authentication server (authsvr) running.

5. In the PORT # field, enter the port number to connect with on the remote host.

6. (Optional) To specify a command that enables you to connect with the remote server, enter the command in the PROXY COMMAND field. You should only specify a proxy command if it is required by the server. The command string is executed with /bin/sh. The command should read from its stdin and write to its stdout.

7. Select or clear the USE PRIVILEGED PORT check box to indicate whether to use a privileged or non-privileged port for SSH communications. Select the check box to use a privileged port, or clear it to use a non-privileged port. Non-privileged ports can be used to bypass some firewalls that do not allow privileged source ports to pass. If you use a non-privileged port, you cannot select the RHOSTS check box (discussed in *Step 4*).

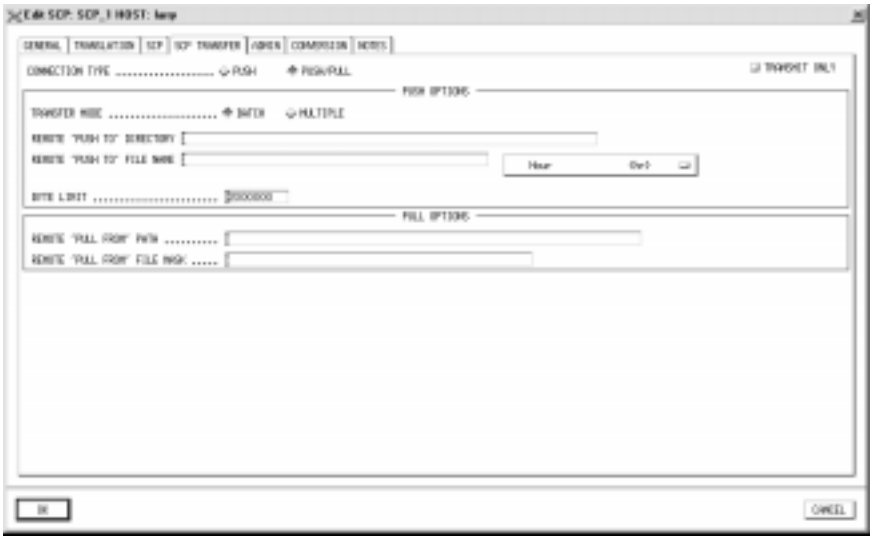
8. Select or clear the SEND ‘KEEPALIVE’ MESSAGES check box to indicate whether to send TCP keepalive messages. Select the check box to send TCP keepalive messages, or clear it if you do not wish to send keepalive messages. If this option is selected, it is possible to detect network outages and automatically close connections.

9. To save your changes, click OK. The changes will go into effect when the next communications session is initiated.

To view and edit SCP transfer parameters

1. In the edit channel window, click the SCP TRANSFER tab.

Figure B-3 Edit Channel Window: SCP Transfer Tab



2. To specify the connection protocol for the channel, select one of the CONNECTION TYPE option buttons:

   - PUSH is a send-only protocol. If this option button is selected, ECPN only transmits messages to the specified “in” directory on the remote host, as indicated in the REMOTE ‘PUSH TO’ DIRECTORY field.

   - PUSH/PULL is a send-and-receive protocol. If this option button is selected, ECPN transmits messages to the specified “in” directory of the remote host (as indicated in the REMOTE ‘PUSH TO’ DIRECTORY field) and retrieves any waiting messages from the specified “out” directory of the remote host. If the “in” and “out” directories are the same, you must enter filter information in the REMOTE ‘PULL FROM’ FILE MASK field (as described in *Step 9*).

3. Select or clear the TRANSMIT ONLY check box to set the communication mode for the channel. When this check box is selected, the channel sends messages but does not receive them. When this check box is cleared, the channel returns to the setting in place (push or push/pull) before the transmit-only mode was activated.

4. In the PUSH OPTIONS box, select one of the TRANSFER MODE option buttons to specify the mode of file transfer:

   - BATCH – Transfers one or more messages per file, depending on the variable(s) included in the file name of each message. For information on variables, see *Step 6* in *To view and edit FTP transfer parameters* in the *Software User's Guide for Electronic Commerce Processing Node*.

   - MULTIPLE – Transfers one message per file.

   NOTE: All administrative messages sent by ECPN (i.e., traffic reports and 824 or 997 acknowledgments) are transferred as one message per file, regardless of the TRANSFER mode set.

5. In the REMOTE 'PUSH TO' DIRECTORY field, enter the path on the remote host to which ECPN should push files. The path entered may be absolute or relative to the remote login directory. If this field is left blank, the files will be pushed to the login directory.

6. In the REMOTE 'PUSH TO' FILE NAME field, enter the file name on the remote host to which ECPN should push files. For information on entering a file name, see *Step 6* in *To view and edit FTP transfer parameters* in the *Software User's Guide for Electronic Commerce Processing Node*.

7. For batch mode file transfers, enter the byte size of data that you wish to transmit at a time in the BYTE LIMIT field. The default value is 20000, indicating the message will be transmitted in chunks of 2 MB. Note that this field is unavailable for multiple mode.

8. In the REMOTE 'PULL FROM' PATH field, enter the path on the remote host from which ECPN should pull files. The path entered may be absolute or relative to the remote login directory. You must end this entry with the path delimiter required by the remote host. Other than verifying that the last character in the entry is non-alphanumeric, error checking does not occur. Note that if this field does not contain an entry, an attempt is made to pull the files from the remote login directory.

9. In the REMOTE 'PULL FROM' FILE MASK field, enter the name of the file(s) to be pulled from the remote host. An entry is required if the channel is pushing to and pulling from the same directory. Otherwise, the channel will pull back the files that it just transmitted.

You may use wildcards (discussed in Section 1.3 of the *Software User's Guide for Electronic Commerce Processing Node*) in this field to pull a combination of files at once. For example, suppose the remote site uses the file name extension .out to signify which files should be pulled. To pull only those files that end with .out from the remote pull from directory, you should enter the wildcard *.out in the REMOTE 'PULL FROM' FILE MASK field. Files not ending with the .out extension are ignored.

This page has been intentionally left blank.